

Jason Lescelius

From: Kristina Temel
Sent: Tuesday, 16 April 2019 2:03 PM
To: Benjamin Baker
Subject: FW: Cyber security information for political party secretaries
Attachments: Cyber security

Ben,

Michael has come back to confirm that what we provided in 2017 needs no update and is still current. We could include this in the next party secretary update.

KT



Make your voice heard.
Enrol now 

ELECTIONS

Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

From: Kristina Temel
Sent: Tuesday, 16 April 2019 8:39 a.m.
To: 6(a)
Subject: RE: Cyber security information for political party secretaries

Hi 6(a)

Here is a copy of what was sent to parties.

Kind regards

Kristina



Make your voice heard.
Enrol now 

ELECTIONS

Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

From: 6(a)
Sent: Monday, 15 April 2019 2:20 p.m.
To: Kristina Temel
Subject: RE: Cyber security information for political party secretaries

Hi Kristina,

I have reviewed the content we provided and at this stage do not believe there any updates required.

I have been reviewing a version we have stored in our system – could you please send through the version you refer to in your original email?

I just want to 100% confirm there aren't any differences before finalising.

Thanks,

6(a)



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

From: Kristina Temel [mailto:kristina.temel@Elections.govt.nz]

Sent: Tuesday, 9 April 2019 10:42 a.m.

To: 6(a)

Subject: RE: Cyber security information for political party secretaries

Hi 6(a)

Thank you for your email.

Look forward to your response.

Kind regards

Kristina



Make your voice heard.

Enrol now 

ELECTIONS

Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

From: 6(a)

Sent: Tuesday, 9 April 2019 10:10 a.m.

To: Kristina Temel
Subject: RE: Cyber security information for political party secretaries

Hi Kristina,

Thanks for your time on the phone today. I am emailing you so you have my contact details should you need anything further.

As discussed, we will review the content provided and let you know if any changes need to be made.

I will be in touch in the coming days.

Thanks.

6(a)



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

From: Kristina Temel [mailto:kristina.temel@Elections.govt.nz]
Sent: Thursday, 28 February 2019 9:53 a.m.
To: Lisa Fong
Cc: Alicia Wright
Subject: Cyber security information for political party secretaries

Hi Lisa,

Given the recent announcement by the Australian Prime Minister that the IT networks of the country's major political parties had been compromised by a "sophisticated state actor", we think it would be timely to provide party secretaries tips about best practice and contacts for agencies they can go to for advice and assistance to protect themselves and/or report any incidents.

I have attached the information that we provided to party secretaries before the 2017 General Election. It would be great if you could review this and provide any suggested updates.

We have had some new party secretaries appointed and it would be good to ensure that these issues are highlighted well in advance of the election.

We are aiming to send this out as part of a quarterly update for party secretaries along with other information that is of interest about electoral developments and preparations for the election. The next quarterly update is due to go out in the next 6-8 weeks.

Happy to discuss further

Kind regards

Kristina Temel



Make your voice heard.

Enrol now 



Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

CONFIDENTIALITY NOTICE: This e-mail message and attachments do not necessarily reflect the views of the New Zealand Electoral Commission and may contain information that is confidential and may be subject to legal privilege. If you are not the intended recipient, you are hereby notified that you must not use, disseminate, distribute or copy this e-mail message or its attachments. If you received this message in error, please notify the Electoral Commission by telephone (call collect: 00-64-4-495-0030) or return the original message to us by e-mail, and destroy any copies. Thank you.

This electronic message, together with any attachments, contains information that is provided in confidence and may be subject to legal privilege. Any classification markings must be adhered to. If you are not the intended recipient, you must not peruse, disclose, disseminate, copy or use the message in any way. If you have received this message in error, please notify us immediately by return email and then destroy the original message. The New Zealand Intelligence Community (NZIC) and the departments comprising the NZIC accepts no responsibility for changes to this e-mail, or to any attachments, after its transmission from NZIC. This communication may be accessed or retained for information assurance purposes. Thank you.

This email has been filtered by SMX. For more information visit smxemail.com

CONFIDENTIALITY NOTICE: This e-mail message and attachments do not necessarily reflect the views of the New Zealand Electoral Commission and may contain information that is confidential and may be subject to legal privilege. If you are not the intended recipient, you are hereby notified that you must not use, disseminate, distribute or copy this e-mail message or its attachments. If you received this message in error, please notify the Electoral Commission by telephone (call collect: 00-64-4-495-0030) or return the original message to us by e-mail, and destroy any copies. Thank you.

This electronic message, together with any attachments, contains information that is provided in confidence and may be subject to legal privilege. Any classification markings must be adhered to. If you are not the intended recipient, you must not peruse, disclose, disseminate, copy or use the message in any way. If you have received this message in error, please notify us immediately by return email and then destroy the original message. The New Zealand Intelligence Community (NZIC) and the departments comprising the NZIC accepts no responsibility for changes to this e-mail, or to any attachments, after its transmission from NZIC. This communication may be accessed or retained for information assurance purposes. Thank you.

This email has been filtered by SMX. For more information visit smxemail.com

Jason Lescelius

From: Kristina Temel
Sent: Monday, 22 May 2017 5:29 PM
To: Kristina Temel
Cc: Alicia Wright
Subject: Cyber security

Dear Party Secretary,

Recent events overseas remind us that politicians, political parties, and public sector agencies can be targeted online and need to be mindful of cyber security. Below are some general points on security steps that we can all put in place to protect ourselves online and to avoid unauthorised access to personal information and our systems.

- **Digital footprint**

Whenever you use the internet or other people publish information about you or your activities online, it leaves behind a footprint that may help others identify your interests, activities or locations you regularly attend. Use a search engine to review what information is already out there about you online and review the sensitivity of that data.

- **Think before you share**

Both personal and company/organisation information can have intrinsic value to people looking for ways to exploit systems or get access to places they shouldn't be allowed. Consider carefully every request by email, text or phone for sensitive data that shouldn't be shared widely. Social media platforms can also be a treasure trove of information so make use of privacy settings to lock down access.

- **Use strong passwords**

Passwords remain a sore point for end users struggling to remember a growing array of logins but are highly after sought by attackers. Complexity through mixing characters sets or overall passphrase length can help defend against determined attacks. Best practice is to never use the same password for more than one account or system and avoid sharing them. Investigate password manager software to help you create and store strong passwords that are too hard to remember.

- **Turn on two-factor authentication**

Multi-factor authentication offers more security over a simple password and requires an attacker to know both your password and have access to your phone or a hardware token that must be used to login. Many companies now offer this form of increased security at no extra cost and layering your defences can be beneficial.

- **Travel securely**

Your travel movements may also be of interest to other people keen to monitor your activities. Avoid posting information online that signals you will be away from your home or office for a long period of time, attackers may see an upcoming foreign trip as the perfect opportunity to access that location or send spoof emails to friends or colleagues that coincide with you being overseas. Avoid taking sensitive information on devices when you travel and be aware that leaving location services turned on may give away your location when using certain mobile apps.

- **Patch, patch and patch again**

Keep your systems and software up to date to address emerging vulnerabilities; automate updates where feasible or apply patches as soon as you can. Surfing the internet with an old web browser can leave you open to attacks such as 'drive-by downloads' or 'malvertising' that let an attacker gain a foothold on your computer for further exploitation. Disable untrusted Microsoft Office macros as this software feature can be used to download malware.

- **Back up important data**
Technology has improved over the years, but creating copies of your essential information can protect you against system failures or data being encrypted via ransomware and ensures you still have access to your files. Storing information both offline and in the cloud can provide a belt and braces approach to give you a range of options if the worst happens.
- **Hold onto your hardware**
Losing a laptop or smartphone is one of the most common ways for data or credentials to be compromised and it can cost significant sums to replace items too. Password protecting devices and using encryption methods to scramble the data stored within them can prevent your information from being accessed if they fall into the wrong hands. Smartphones often come with ways to track and/or remotely wipe them if they are lost or stolen and there are similar tools you can use to protect larger computers.
- **Restrict admin privileges**
An administrative user on a system can add or remove software and may also give permissions to programmes to perform unwanted actions that could, for example, allow an attacker to remotely access your data or view your webcam. Use an admin level account to maintain the computer but create a basic level login to use when simply checking email or browsing the web.
- **Be careful using free Wi-Fi**
A mobile worker needs to access information anywhere and everywhere and free Wi-Fi can be a tempting way to trim data costs when travelling. Unsecure networks may reduce the security of your communications though and it's important not to access sensitive systems or send private messages over insecure connections. Consider a VPN solution to add a protective layer that prevents your data from being intercepted.

There are several organisations who can provide advice and assistance to help keep you and your information secure online. They include the recently established CERT NZ, the National Cyber Security Centre and Netsafe.

CERT NZ can be contacted by phone on 0800 CERT NZ (0800 2378 69) - <https://www.cert.govt.nz>. They provide a central point of contact for reporting cyber incidents and advice on how to protect yourself and your systems from most cyber threats.

The National Cyber Security Centre (NCSC) can be contacted by email to info@ncsc.govt.nz or by phone on 04 498 7654 - <https://www.ncsc.govt.nz>. The NCSC is part of the Government Communications Security Bureau. Its focus is on helping to protect New Zealand's most significant organisations and systems, through the provision of information security guidance, standards, and support in the management of significant cyber security incidents.

Netsafe can be contacted by email to queries@netsafe.org.nz or by phone on 0508 NETSAFE (0508 638 723) - <https://www.netsafe.org.nz>. Netsafe provides a range of information and advice on protecting yourself from more common forms of cyber threat.

Hope you find this of assistance.

Kind regards

Kristina Temel



Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

***** CONFIDENTIALITY
NOTICE: This e-mail message and attachments do not necessarily reflect the views of the New Zealand Electoral Commission and may contain information that is confidential and may be subject to legal privilege. If you are not the intended recipient, you are hereby notified that you must not use, disseminate, distribute or copy this e-mail message or its attachments. If you received this message in error, please notify the Electoral Commission by telephone (call collect: 00-64-4-495-0030) or return the original message to us by e-mail, and destroy any copies. Thank you. *****

Jason Lescelius

From: Kristina Temel
Sent: Tuesday, 4 February 2020 6:31 PM
To: 6(a)
Subject: RE: Cyber security information for political party secretaries
Attachments: FW: Cyber security information for political party secretaries; Party Secretary update - issue 3 May 2019.pdf

Hi 6(a)

I have attached the e-mails so you can see how this progressed and resulted in a May 2019 update sent to all party secretaries.

We didn't get any feedback.

I guess we could repeat again before the GE but it might depend on whether there is any change or update to give them. Happy to take your advice on this.

Kind regards

Kristina

From: 6(a)
Sent: Tuesday, 4 February 2020 4:30 PM
To: Kristina Temel <Kristina.Temel@elections.govt.nz>
Subject: FW: Cyber security information for political party secretaries

Good afternoon Kristina

I have been asked to contact you and introduce myself as 6(a)

In the interim since last February, the attached information you mention has been separated and I wondered if you could resend it to me.

I would also be keen to know how it was received and any other feedback from the exercise.

If you have plans to repeat this exercise again for the upcoming election, I am available as a point of contact at the NCSC and can provide advice or assistance as required.

Cheers

6(a)



**GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU**
TE TIRA TIAKI

From: Kristina Temel [<mailto:kristina.temel@Elections.govt.nz>]
Sent: Thursday, 28 February 2019 9:53 a.m.
To: Lisa Fong
Cc: Alicia Wright
Subject: Cyber security information for political party secretaries

Hi Lisa,

Given the recent announcement by the Australian Prime Minister that the IT networks of the country’s major political parties had been compromised by a “sophisticated state actor”, we think it would be timely to provide party secretaries tips about best practice and contacts for agencies they can go to for advice and assistance to protect themselves and/or report any incidents.

I have attached the information that we provided to party secretaries before the 2017 General Election. It would be great if you could review this and provide any suggested updates.

We have had some new party secretaries appointed and it would be good to ensure that these issues are highlighted well in advance of the election.

We are aiming to send this out as part of a quarterly update for party secretaries along with other information that is of interest about electoral developments and preparations for the election. The next quarterly update is due to go out in the next 6-8 weeks.

Happy to discuss further

Kind regards

Kristina Temel



Make your voice heard.
Enrol now



Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

CONFIDENTIALITY NOTICE: This e-mail message and attachments do not necessarily reflect the views of the New Zealand Electoral Commission and may contain information that is confidential and may be subject to legal privilege. If you are not the intended recipient, you are hereby notified that you must not use, disseminate, distribute or copy this e-mail message or its attachments. If you received this message in error, please notify the Electoral Commission by telephone (call collect: 00-64-4-495-0030) or return the

original message to us by e-mail, and destroy any copies. Thank you.

This electronic message, together with any attachments, contains information that is provided in confidence and may be subject to legal privilege. Any classification markings must be adhered to. If you are not the intended recipient, you must not peruse, disclose, disseminate, copy or use the message in any way. If you have received this message in error, please notify us immediately by return email and then destroy the original message. The New Zealand Intelligence Community (NZIC) and the departments comprising the NZIC accepts no responsibility for changes to this e-mail, or to any attachments, after its transmission from NZIC. This communication may be accessed or retained for information assurance purposes. Thank you.

Jason Lescelius

From: Kristina Temel
Sent: Monday, 22 May 2017 5:29 PM
To: Kristina Temel
Cc: Alicia Wright
Subject: Cyber security

Dear Party Secretary,

Recent events overseas remind us that politicians, political parties, and public sector agencies can be targeted online and need to be mindful of cyber security. Below are some general points on security steps that we can all put in place to protect ourselves online and to avoid unauthorised access to personal information and our systems.

- **Digital footprint**

Whenever you use the internet or other people publish information about you or your activities online, it leaves behind a footprint that may help others identify your interests, activities or locations you regularly attend. Use a search engine to review what information is already out there about you online and review the sensitivity of that data.

- **Think before you share**

Both personal and company/organisation information can have intrinsic value to people looking for ways to exploit systems or get access to places they shouldn't be allowed. Consider carefully every request by email, text or phone for sensitive data that shouldn't be shared widely. Social media platforms can also be a treasure trove of information so make use of privacy settings to lock down access.

- **Use strong passwords**

Passwords remain a sore point for end users struggling to remember a growing array of logins but are highly after sought by attackers. Complexity through mixing characters sets or overall passphrase length can help defend against determined attacks. Best practice is to never use the same password for more than one account or system and avoid sharing them. Investigate password manager software to help you create and store strong passwords that are too hard to remember.

- **Turn on two-factor authentication**

Multi-factor authentication offers more security over a simple password and requires an attacker to know both your password and have access to your phone or a hardware token that must be used to login. Many companies now offer this form of increased security at no extra cost and layering your defences can be beneficial.

- **Travel securely**

Your travel movements may also be of interest to other people keen to monitor your activities. Avoid posting information online that signals you will be away from your home or office for a long period of time, attackers may see an upcoming foreign trip as the perfect opportunity to access that location or send spoof emails to friends or colleagues that coincide with you being overseas. Avoid taking sensitive information on devices when you travel and be aware that leaving location services turned on may give away your location when using certain mobile apps.

- **Patch, patch and patch again**

Keep your systems and software up to date to address emerging vulnerabilities; automate updates where feasible or apply patches as soon as you can. Surfing the internet with an old web browser can leave you open to attacks such as 'drive-by downloads' or 'malvertising' that let an attacker gain a foothold on your computer for further exploitation. Disable untrusted Microsoft Office macros as this software feature can be used to download malware.

- **Back up important data**
Technology has improved over the years, but creating copies of your essential information can protect you against system failures or data being encrypted via ransomware and ensures you still have access to your files. Storing information both offline and in the cloud can provide a belt and braces approach to give you a range of options if the worst happens.
- **Hold onto your hardware**
Losing a laptop or smartphone is one of the most common ways for data or credentials to be compromised and it can cost significant sums to replace items too. Password protecting devices and using encryption methods to scramble the data stored within them can prevent your information from being accessed if they fall into the wrong hands. Smartphones often come with ways to track and/or remotely wipe them if they are lost or stolen and there are similar tools you can use to protect larger computers.
- **Restrict admin privileges**
An administrative user on a system can add or remove software and may also give permissions to programmes to perform unwanted actions that could, for example, allow an attacker to remotely access your data or view your webcam. Use an admin level account to maintain the computer but create a basic level login to use when simply checking email or browsing the web.
- **Be careful using free Wi-Fi**
A mobile worker needs to access information anywhere and everywhere and free Wi-Fi can be a tempting way to trim data costs when travelling. Unsecure networks may reduce the security of your communications though and it's important not to access sensitive systems or send private messages over insecure connections. Consider a VPN solution to add a protective layer that prevents your data from being intercepted.

There are several organisations who can provide advice and assistance to help keep you and your information secure online. They include the recently established CERT NZ, the National Cyber Security Centre and Netsafe.

CERT NZ can be contacted by phone on 0800 CERT NZ (0800 2378 69) - <https://www.cert.govt.nz>. They provide a central point of contact for reporting cyber incidents and advice on how to protect yourself and your systems from most cyber threats.

The National Cyber Security Centre (NCSC) can be contacted by email to info@ncsc.govt.nz or by phone on 04 498 7654 - <https://www.ncsc.govt.nz>. The NCSC is part of the Government Communications Security Bureau. Its focus is on helping to protect New Zealand's most significant organisations and systems, through the provision of information security guidance, standards, and support in the management of significant cyber security incidents.

Netsafe can be contacted by email to queries@netsafe.org.nz or by phone on 0508 NETSAFE (0508 638 723) - <https://www.netsafe.org.nz>. Netsafe provides a range of information and advice on protecting yourself from more common forms of cyber threat.

Hope you find this of assistance.

Kind regards

Kristina Temel



Kristina Temel | Manager Legal and Policy | Electoral Commission | Te Kaitiaki Take Kōwhiri PO Box 3220 | Level 10, 34-42 Manners Street | Wellington Phone +64 4 806 3506 | Fax +64 4 495 0031 | <http://www.elections.org.nz>

***** CONFIDENTIALITY

NOTICE: This e-mail message and attachments do not necessarily reflect the views of the New Zealand Electoral Commission and may contain information that is confidential and may be subject to legal privilege. If you are not the intended recipient, you are hereby notified that you must not use, disseminate, distribute or copy this e-mail message or its attachments. If you received this message in error, please notify the Electoral Commission by telephone (call collect: 00-64-4-495-0030) or return the original message to us by e-mail, and destroy any copies. Thank you. *****

Party Secretary Update

Issue 3, May 2019

KIA ORA

Welcome to issue 3. We want to make sure you are well equipped to protect your party from cyber security threats. Page 2 sets out advice on the practical steps you can put in place to avoid unauthorised access to your systems. This advice was last circulated prior to the 2017 election and we hope will be particularly helpful to those of you who have taken on the party secretary role since the election. We have had a couple of announcements in recent weeks that mean we now have greater certainty about the timing of the boundary review, starting later this year, as well as next year's referendum on recreational cannabis use. Read on to find out more on these topics and other electoral-related matters being considered by Parliament. Please get in touch if there are any subjects you would like us to cover off in future issues.

Kristina Temel
Manager Legal and Policy



IN THIS ISSUE

Cyber security and political parties
General Election 2020 and cannabis referendum
Justice Select Committee Inquiry into 2017 General Election and 2016 Local Elections
Legislation update
2019 boundary review
Party news
Website news

Contact details

Electoral Commission head office:
Level 10, 34-42 Manners Street, Wellington, 6140
Telephone: 04 495 0030
Websites: www.elections.org.nz www.electionresults.govt.nz

General enquiries: enquiries@elections.govt.nz
Advisory opinion requests: advisory@elections.govt.nz
Requests for roll data: data@elections.govt.nz

Cyber security and political parties

Recent events overseas remind us that politicians, political parties, and public sector agencies can be targeted online and need to be mindful of cyber security. Below are some general points on security steps that we can all put in place to protect ourselves online and to avoid unauthorised access to personal information and our systems.

Digital footprint

Whenever you use the internet or other people publish information about you or your activities online, it leaves behind a footprint that may help others identify your interests, activities or locations you regularly attend. Use a search engine to review what information is already out there about you online and review the sensitivity of that data.

Think before you share

Both personal and company/organisation information can have intrinsic value to people looking for ways to exploit systems or get access to places they shouldn't be allowed. Consider carefully every request by email, text or phone for sensitive data that shouldn't be shared widely. Social media platforms can also be a treasure trove of information so make use of privacy settings to lock down access.

Use strong passwords

Passwords remain a sore point for end users struggling to remember a growing array of logins but are highly sought after by attackers. Complexity through mixing characters sets or overall passphrase length can help defend against determined attacks. Best practice is to never use the same password for more than one account or system and avoid sharing them. Investigate password manager software to help you create and store strong passwords that are too hard to remember.

Turn on two-factor authentication

Multi-factor authentication offers more security over a simple password and requires an attacker to know both your password and have access to your phone or a hardware token that must be used to login. Many companies now offer this form of increased security at no extra cost and layering your defences can be beneficial.

Travel securely

Your travel movements may also be of interest to other people keen to monitor your activities. Avoid posting

information online that signals you will be away from your home or office for a long period of time, attackers may see an upcoming foreign trip as the perfect opportunity to access that location or send spoof emails to friends or colleagues that coincide with you being overseas. Avoid taking sensitive information on devices when you travel and be aware that leaving location services turned on may give away your location when using certain mobile apps.

Patch, patch and patch again

Keep your systems and software up to date to address emerging vulnerabilities; automate updates where feasible or apply patches as soon as you can. Surfing the internet with an old web browser can leave you open to attacks such as 'drive-by downloads' or 'malvertising' that let an attacker gain a foothold on your computer for further exploitation. Disable untrusted Microsoft Office macros as this software feature can be used to download malware.

Back up important data

Technology has improved over the years, but creating copies of your essential information can protect you against system failures or data being encrypted via ransomware and ensures you still have access to your files. Storing information both offline and in the cloud can provide a belt and braces approach to give you a range of options if the worst happens.

Hold onto your hardware

Losing a laptop or smartphone is one of the most common ways for data or credentials to be compromised and it can cost significant sums to replace items too. Password protecting devices and using encryption methods to scramble the data stored within them can prevent your information from being accessed if they fall into the wrong hands. Smartphones often come with ways to track and/or remotely wipe them if they are lost or stolen and there are similar tools you can use to protect larger computers.

Restrict admin privileges

An administrative user on a system can add or remove software and may also give permissions to programmes to perform unwanted actions that could, for example, allow an attacker to remotely access your data or view your webcam. Use an admin level account to maintain the computer but create a basic level login to use when simply checking email or browsing the web.

Be careful using free Wi-Fi

A mobile worker needs to access information anywhere and everywhere and free Wi-Fi can be a tempting way to trim data costs when travelling. Unsecure networks may reduce the security of your communications though and it's important not to access sensitive systems or send private messages over insecure connections. Consider a VPN solution to add a protective layer that prevents your data from being intercepted.

There are several organisations who can provide advice and assistance to help keep you and your information secure online. They include the recently established CERT NZ, the National Cyber Security Centre and Netsafe.

CERT NZ can be contacted by phone on 0800 CERT NZ (0800 2378 69) - <https://www.cert.govt.nz>. They provide a central point of contact for reporting cyber incidents and advice on how to protect yourself and your systems from most cyber threats.

The National Cyber Security Centre (NCSC) can be contacted by email to info@ncsc.govt.nz or by phone on 04 498 7654 - <https://www.ncsc.govt.nz>. The NCSC is part of the Government Communications Security Bureau. Its focus is on helping to protect New Zealand's most significant organisations and systems, through the provision of information security guidance, standards, and support in the management of significant cyber security incidents.

Netsafe can be contacted by email to queries@netsafe.org.nz or by phone on 0508 NETSAFE (0508 638 723) - <https://www.netsafe.org.nz>. Netsafe provides a range of information and advice on protecting yourself from more common forms of cyber threat.



General Election 2020 and cannabis referendum

On 7 May 2019, the Government announced the format of the referendum on legalising personal use of cannabis to be held alongside the 2020 General Election. The Government confirmed voters will be able to vote 'yes' or 'no' on a draft bill that sets out the way recreational use of cannabis could be legalised and regulated. The bill could be considered by the next Parliament if voters choose 'yes'.

Legislation will need to be passed this term for the actual delivery of that referendum. This will also cover any rules about advertising and campaigning in relation to the referendum topic.

We are underway with preparations to deliver both the General Election and any referendums held with it. Our first voting simulations, held in April, were a success. We tested the time and staff needed to issue both the general election and referendum ballot papers to voters. This will be valuable information as we work to ensure the smooth delivery of the election and implement any legislative and operational changes.

Justice Select Committee Inquiry into 2017 General Election and 2016 Local Elections

On 15 March 2019 the election inquiry reopened submissions so that the Justice Committee could specifically consider how New Zealand can protect its democracy from inappropriate foreign interference. Submissions have now closed and the Committee is considering these issues. In particular it is examining:

- the ability of foreign powers to hack the emails of parties and candidates
- the risk that political campaigns on social media can be made to appear domestic when they are actually driven by external entities, and
- the risk that donations to political parties are made by foreign governments or entities.

You can continue to follow progress [here](#).

After the Inquiry concludes, the Government may advance any changes to electoral law through a bill to be passed in 2020.

Legislation update

The [Local Electoral Matters Act](#), mentioned in our previous updates, received royal assent on 8 April 2019.

The report back of the [Election Access Fund Bill](#) is now due on 24 June 2019. Additional time has been allowed in select committee for policy considerations by the Governance and Administration Committee. This member's Bill proposes an Election Access Fund to be available to any disabled candidate, not-for-profit bodies, and registered political parties. You can find out more and follow progress on the Bill [here](#).

The [Electoral \(Entrenchment of Māori Seats Amendment Bill\)](#) is currently before the Māori Affairs Select Committee. This is another member's Bill, which is to entrench the provisions of the Electoral Act 1993 that relate to the Māori electorates. You can follow progress [here](#).

2019 boundary review

On 29 April the Government Statistician confirmed the first release of 2018 Census data will be on 23 September 2019. This will include the number of electorates for the 2020 and 2023 General Elections and the electoral populations for the boundary review.

On this basis we expect the boundary review to run from October to April next year, which will be the same as the timeline in 2013/14.

The Representation Commission approves the timetable when it first meets. At this stage we expect the timetable to be as follows:

- October - deliberations on the proposed boundaries
- November - proposed boundaries released for public comment (one month minimum period for objections)
- January - counter-objection period (2 week minimum period)
- February - public hearings and deliberations on final boundaries
- April - final boundaries presented to Governor-General and Parliament



We will be providing secretariat and administrative support to the Representation Commission, with technical support provided by Statistics NZ and LINZ.

At the beginning of the process parliamentary parties and independent MPs have the opportunity to submit to the Representation Commission on matters to be considered by the Commission in their determination of the boundaries.

All parties have the opportunity to have their say on the proposed boundaries and the names of the electorates by making objections or counter-objections.

Party news

30 April 2019 marked the deadline for political parties to submit their annual return of donations and loans, as well as the annual declaration under section 71A of the Electoral Act. We thank all parties for ensuring these documents were received on time. On 2 May 2019 the returns were published on the Commission's website.

One party has sought deregistration since the last update. The New Zealand People's Party was cancelled by the Electoral Commission on 30 April 2019.

There are currently 12 registered parties. We have no party or logo registration applications at the moment.

Website news

The Commission will launch two new websites in June.

www.vote.nz will be a simple transactional site for people wanting to enrol or get information on how to vote.

www.elections.nz will hold more detail, including the rules and requirements for parties and the information about New Zealand's democracy currently found on our current website.

The websites will be ready for the Commission's enrolment update campaign for the local body elections later this year.

After the sites go live there will be a phased approach to adding more content as we get closer to the 2020 General Election.